J1033 U.S. PTO
09/784719
02/14/01

대 한 민 국 특 허 청

KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 32182 호
Application Number

출 원 년 월 일 : 2000년 06월 12일
Date of Application

출 원 인 : 주식회사 퓨쳐시스템
Applicant(s)

CERTIFIED COPY OF PRIORITY DOCUMENT

2000 년 08 월 28 일

특 허 청
COMMISSIONER

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2000.06.12
【발명의 명칭】	통합형 보안 게이트웨이를 구비한 네트워크 시스템
【발명의 영문명칭】	Network system with integrated security gateway
【출원인】	
【명칭】	주식회사 퓨쳐시스템
【출원인코드】	1-1998-004100-4
【대리인】	
【성명】	이정익
【대리인코드】	9-1998-000410-4
【포괄위임등록번호】	2000-006349-7
【발명자】	
【성명의 국문표기】	김광태
【성명의 영문표기】	KIM,Kwang tae
【주민등록번호】	591203-1540629
【우편번호】	463-030
【주소】	경기도 성남시 분당구 분당동 113 건영빌라 302동 106호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 이정익 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	5 면 5,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	8 항 365,000 원
【합계】	399,000 원
【감면사유】	중소기업
【감면후 수수료】	199,500 원
【첨부서류】	1. 요약서·명세서(도면)_1통 2.중소기업법시행령 제2조에의한 중소기업에 해당함을 증명하는 서류 _1통

【요약서】

【요약】

본 발명은 통합형 보안 게이트웨이를 구비한 네트워크 시스템에 관한 것으로, 적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와; 상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와; 상기 내부 네트워크와 상기 외부 네트워크를 연결하기 위한 라우터와; 상기 외부 네트워크를 경유한 외부 침입으로부터 상기 내부 네트워크의 자원을 보호하기 위한 방화벽 기능 및 게이트웨이 기능을 제공하기 위하여, 상기 라우터와 상기 내부 네트워크 사이에 설치된 통합형 보안 게이트웨이와; 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지하는 침입 탐지 수단을 구비하고 있고, 여기서 상기 침입 탐지 수단은 내부 및 외부에서 자신의 존재 여부가 탐지되지 않도록 네트워크 영역에 위치되어 있다.

【대표도】

도 4

【색인어】

내부 네트워크, 외부 침입, 방화벽, 게이트웨이, 침입 탐지, 네트워크 영역

【명세서】

【발명의 명칭】

통합형 보안 게이트웨이를 구비한 네트워크 시스템{Network system with integrated security gateway}

【도면의 간단한 설명】

도 1은 종래의 방화벽을 구비한 네트워크 시스템의 구성도.

도 2는 종래의 방화벽을 구비한 다른 네트워크 시스템의 구성도.

도 3은 종래의 방화벽과 네트워크 모니터링 시스템을 구비한 네트워크 시스템의 구성도.

도 4는 본 발명의 바람직한 실시예에 따른 통합형 보안 게이트웨이를 구비한 네트워크 시스템의 구성도.

도 5는 도 4에 도시된 통합형 보안 게이트웨이의 배면도.

도 6은 도 4에 도시된 통합형 보안 게이트웨이에서의 패킷의 흐름도.

* 도면의 주요 부분에 대한 부호의 설명

400 : 내부 네트워크 410 : 서버

420a, 420b : 클라이언트 430 : 통합형 보안 게이트웨이

440 : 라우터 450 : 외부 네트워크

460 : 네트워크 모니터링 시스템

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<12> 본 발명은 보안 장치가 구축된 네트워크 시스템에 관한 것으로, 특히 게이트웨이 기능, 방화벽 기능, 및 침입 탐지 기능을 제공하기 위한 통합형 보안 게이트웨이를 구비한 네트워크 시스템에 관한 것이다.

<13> 일반적으로, 방화벽(firewall)은 네트워크 게이트웨이 서버에 위치하고 있는 프로그램으로서, 인터넷과 같은 외부 네트워크 상의 사용자들로부터 내부 네트워크(예컨대, 가상 사설망(Virtual Private Network ; VPN))의 공개되지 않은 자원을 보호하고, 내부 네트워크 상의 사용자들이 외부 네트워크 상의 자원에 접근하는 것을 통제하는데 사용된다. 방화벽은 입력 네트워크 패킷이 내부 네트워크로 바로 전달되지 않도록 라우터와 밀접하게 동작하여, 모든 네트워크 패킷을 내부 네트워크로 전달할 것인지를 결정하기 위해 상기 네트워크 패킷을 검사한다.

<14> 방화벽의 차단 방법에는 여러 가지가 있다. 단순한 방법 중 하나는 입력 네트워크 패킷이 받아들일만한(즉, 이전에 확인된) 도메인 이름이나 IP 주소로부터 입력되는 것인지를 확인하는 방법이다. 이동중인 사용자들은 보안 접속 절차나 인증 확인 등을 통해 내부 네트워크에 원격 접속할 수 있다. 방화벽 제품들을 만드는 회사들도 꽤 있다. 방화벽에 포함되어야할 기능으로는, 사용기록, 보고, 공격이 시작된 시점에서의 자동경보, 그리고 방화벽의 제어를 위한 그래픽사용자 인터페이스 등이 있다.

<15> 가상 사설망은 공중 통신망 기반시설을 터널링 프로토콜과 보안 절차 등을 사용하

여 개별 기업의 목적에 맞게 구성한 데이터 네트워크이다. 가상 사설망은 한 회사에 의해서만 사용될 수 있는 자체망이나 전용 회선과 대비되는 개념이다. VPN은 모든 회사들이 저마다 개별적으로 회선을 임차하는 것보다는 공중망을 공유하여 비용을 낮추면서도 전용회선과 거의 동등한 서비스를 제공하려는 아이디어에서 출발하였다. 전화 회사들은 음성 메시지에 대해 보안이 유지되는 공유자원을 제공한다. 가상 사설망은 데이터를 위해서도 역시 보안이 유지되는 공중망 자원의 공유를 가능하도록 한다. 오늘날 가상 사설망을 원하는 회사들은 주로 엑스트라넷이나 넓은 지역에 퍼져있는 지사들 간의 인트라넷에 이를 이용한다.

<16> 가상 사설망은 공중망을 통해 데이터를 송신하기 전에 데이터를 암호화하고, 수신측에서 복호화한다. 암호화는 데이터뿐 아니라, 부가적인 차원의 보안으로서 송수신지의 네트워크 주소도 포함된다. 마이크로소프트, 3Com 그리고 몇몇 다른 회사들이 PPTP(Point-to-Point Tunneling Protocol)라는 표준 프로토콜을 제안하였으며, 마이크로소프트는 이 프로토콜을 윈도우NT 서버에 내장시켰다. 마이크로소프트의 PPTP와 같은 VPN 소프트웨어는 대개 회사의 방화벽 서버에 설치되는 보안 소프트웨어도 마찬가지로 지원한다.

<17> 이와 같은 종래의 방화벽을 구비한 네트워크 시스템이 도 1에 도시되어 있다. 종래의 네트워크 시스템은 도시된 바와 같이 내부 네트워크(100)와 외부 네트워크(150)를 구비하고 있다. 내부 네트워크(100)는 예컨대 가상 사설 네트워크이고, 외부 네트워크(150)는 인터넷이다. 상기 내부 네트워크(100)는 적어도 하나 이상의 서버(편의상 하나의 서버만이 도시되어 있음)(110)와 복수의 클라이언트(편의상 2 개의 클라이언트만이 도시되어 있음)(120a, 120b)를 구비하고 있다.

<18> 종래의 네트워크 시스템은 또한 상기 내부 네트워크(100)와 상기 외부 네트워크(150)를 상호 연결하기 위한 라우터(140)와, 상기 내부 네트워크(100)와 상기 라우터(140) 사이에 위치된 방화벽(130)을 구비하고 있다. 라우터(140)는 동일한 전송 프로토콜을 사용하는 분리된 네트워크들, 즉 상기 내부 네트워크(100)와 상기 외부 네트워크(150)를 연결하기 위한 장치이다. 방화벽(130)은 외부 네트워크(150) 상의 사용자로부터 내부 네트워크(100)의 자원을 보호하기 위하여, 외부 네트워크(150)의 사용자들이 상기 내부 네트워크(100)의 공개되지 않은 자원에 접근하는 것을 막는 역할을 하며, 도 1에서는 라우터(140)의 뒤에 위치되어 있다. 상기 방화벽은 유사한 기능의 장치에 의해서 대체될 수 있다.

<19> 도 2에는 종래의 방화벽과 네트워크 모니터링 시스템을 구비한 네트워크 시스템이 도시되어 있다. 도 2에서, 종래의 네트워크 시스템은 내부 네트워크(200)와 방화벽(230) 사이에 네트워크 모니터링 시스템(260)을 구비한 것을 제외하고는 도 1의 네트워크 시스템과 실질적으로 동일하다. 따라서, 도 1의 것과 동일한 부분에 대해서는 상세히 설명하지 않는다.

<20> 도 2의 종래 네트워크 시스템에 구비된 네트워크 모니터링 시스템(260)은 외부 네트워크(250)에서 보았을 때 방화벽(230)의 뒤에 설치되어 있으며, 따라서 방화벽(230)을 통과한 네트워크 패킷에 대해서만 침입 여부를 탐지할 수 있고, 방화벽 자체에 대한 직접적인 외부 공격이나 방화벽 앞단에 대한 침입 여부는 탐지할 수 없게 된다.

<21> 즉, 도 2에 도시된 바와 같이, 네트워크 모니터링 시스템(260)을 방화벽(230)의 뒷부분에 설치함으로써 네트워크 모니터링 시스템(260)에 의해 가능한 침입 탐지 범위는 내부 네트워크(200)와 방화벽(230)의 뒷부분 사이, 즉 'a'에 불과하다. 방화벽(230)에

대한 직접적인 외부 공격과, 방화벽(230)의 앞단에 대한 외부 공격은 탐지할 수 없다. 이로 인해, 도 2의 네트워크 시스템에 구비된 방화벽과 네트워크 모니터링 시스템에 의해서는 완전한 보안 정책이 수립될 수 없으며, 특히 방화벽 자체에 대한 외부 공격으로 인해 방화벽이 외부 공격자에게 점유될 경우에는 내부 네트워크가 공격자에게 무방비 상태로 될 수 있는 위험이 있다.

<22> 도 3에는 종래의 방화벽과 네트워크 모니터링 시스템을 구비한 다른 네트워크 시스템이 도시되어 있다. 도 3의 종래의 네트워크 시스템은 방화벽(330)의 앞단에 네트워크 모니터링 시스템(360)이 설치되어 있는 것을 제외하고는 도 2의 네트워크 시스템과 실질적으로 동일하다. 따라서, 도 2의 구성과 동일한 부분에 대해서는 상세히 설명하지 않는다. 도 3에서, 상기 네트워크 모니터링 시스템(360)을 방화벽(33)의 앞단에 설치함으로써 방화벽(330)의 앞단의 침입 여부를 탐지할 수 있다. 따라서, 도 3에 있어서, 네트워크 모니터링 시스템(360)에 의해 가능한 침입 탐지 범위는 방화벽(330)의 앞단에서부터 내부 네트워크(300)까지, 즉 'b'이다. 도 2의 경우와는 달리 침입 탐지 범위가 방화벽의 앞단까지 확대되었음을 알 수 있다. 하지만, 이와 같이 방화벽(330)의 앞단에 네트워크 모니터링 시스템(360)을 설치한 경우에는, 상기 네트워크 모니터링 시스템(360) 자체가 외부 네트워크(350)의 외부 공격자로부터 직접적인 공격 대상이 될 수 있다.

<23> 이와 같이, 종래의 네트워크 시스템에서는, 네트워크 모니터링 시스템이 방화벽의 앞 또는 뒤에 설치되어 있다. 따라서, 방화벽에 대한 직접적인 외부 공격과, 방화벽의 앞단에 대한 외부 공격을 탐지할 수 없어, 완전한 보안 정책이 수립될 수 없으며, 특히 방화벽 자체에 대한 외부 공격으로 인해 방화벽이 외부 공격자에게 점유될 경우에는 내

부 네트워크가 공격자에게 무방비 상태로 될 수 있는 위험이 있다. 또한, 네트워크 모니터링 시스템 자체가 외부 네트워크의 외부 공격자로부터 직접적인 공격 대상이 될 수 있으며, 최악의 경우에는 네트워크 모니터링 시스템이 네트워크 침입을 위한 공격자의 침입 발판이 될 수도 있다.

<24> 또한, 종래의 네트워크 시스템은 게이트웨이, 방화벽, 및 네트워크 모니터링 시스템을 각각 별개의 독립된 장치로 구비하고 있었다. 따라서, 각 장치의 설치 비용이 증가하고, 장치간의 연동성이 저하되며, 연동성 저하로 인해 보안 홀(security hole)이 형성되고, VPN에 대한 연동성이 저하되는 등의 여러 가지 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<25> 본 발명은 상기 종래의 문제점을 해결하기 위한 것으로, 게이트웨이 및 방화벽 기능을 제공하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템을 제공하는데 목적이 있다.

<26> 본 발명의 다른 목적은 게이트웨이, 방화벽, 및 네트워크 모니터링 기능을 제공하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템을 제공하는데 있다.

【발명의 구성 및 작용】

<27> 상기 목적을 달성하기 위하여, 본 발명은 적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와; 상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와; 상기 내부 네트워크와 상기 외부 네트워크를 연결하기 위한 라우터와;

상기 외부 네트워크를 경유한 외부 침입으로부터 상기 내부 네트워크의 자원을 보호하기 위한 방화벽 기능 및 게이트웨이 기능을 제공하기 위하여, 상기 라우터와 상기 내부 네트워크 사이에 설치된 통합형 보안 게이트웨이와; 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지하는 침입 탐지 수단을 구비하고 있고, 상기 침입 탐지 수단은 내부 및 외부에서 자신의 존재 여부가 탐지되지 않는 네트워크 영역(이하, '블랙 존'(black zone)이라고도 함)에 위치되어 있다.

<28> 상기 통합형 보안 게이트웨이는 상기 외부 네트워크로부터의 입력 패킷을 상기 내부 네트워크로 직접 전송하지 않고 방화벽으로 전송하며, 상기 방화벽에서 상기 입력 패킷이 정당 패킷으로 확인될 때 상기 입력 패킷을 복제하여 상기 침입 탐지 수단에 전송함으로써 침입 여부가 이중으로 탐지되도록 한다. 상기 네트워크 영역은 상기 통합형 보안 게이트웨이에 병렬 연결됨으로써 형성된 영역이다.

<29> 본 발명은 적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와; 상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와; 상기 내부 네트워크와 상기 외부 네트워크를 연결하기 위한 라우터와; 상기 외부 네트워크를 경유한 외부 침입으로부터 상기 내부 네트워크의 자원을 보호하기 위한 방화벽 기능, 게이트웨이 기능, 및 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지하는 침입 탐지 기능을 제공하기 위하여, 상기 라우터와 상기 내부 네트워크 사이에 설치된 통합형 보안 게이트웨이를 구비하고 있고, 상기 통합형 보안 게이트웨이의 침입 탐지 기능은 내부 및 외부에서 자신의 존재 여부가 탐지되지 않는 네트워크 영역에서 구현된다.

<30> 상기 내부 네트워크는 가상 사설망(VPN)이고, 상기 외부 네트워크는 인터넷이다.

<31> 상기 통합형 보안 게이트웨이는 내부 및 외부에서 자신의 존재 여부가 탐지되지 않는 네트워크 영역에 위치된 서버 (이하, "블랙 존 서버" (black zone server)이라고도 함) 블랙 존에 연결할 수 있다. 블랙 존 서버 및 허브에 의해 연결된 부가 수단을 통해 침입 차단, 침입 탐지, 바이러스 검사, 유해 사이트 차단 등의 기능을 행한다.

<32> 상기 통합형 보안 게이트웨이는 특정영역(DMZ)에 설치되어 있는 네트워크 장치 및 자원에 대해 외부 침입 차단, 침입 탐지, 바이러스 검사, 유해 사이트 차단 기능 등을 제공한다.

<33> 이하에서는 첨부 도면을 참조하여 본 발명의 바람직한 실시예에 대해 설명한다.

<34> 본 발명의 네트워크 시스템은 도 4에 도시된 바와 같이 내부 네트워크(400)와 외부 네트워크(450)를 구비하고 있다. 내부 네트워크(400)는 가상 사설 네트워크일 수 있고, 외부 네트워크(450)는 인터넷일 수 있다. 상기 내부 네트워크(400)는 적어도 하나 이상의 서버(편의상 하나의 서버만이 도시되어 있음)(410)와 복수의 클라이언트(편의상 2 개의 클라이언트만이 도시되어 있음)(420a, 420b)를 구비하고 있다.

<35> 상기 네트워크 시스템은 또한 상기 내부 네트워크(400)와 상기 외부 네트워크(450)를 연결하는 라우터(440)를 구비하고 있다. 라우터(440)는 동일한 전송 프로토콜을 사용하는 분리된 복수의 네트워크, 즉 도 4에 있어서 상기 내부 네트워크(400)와 상기 외부 네트워크(450)를 연결하기 위한 장치이다.

<36> 본 발명의 네트워크 시스템은 또한 통합형 보안 게이트웨이(430)를 구비하고 있다. 상기 통합형 보안 게이트웨이(430)는 외부 네트워크(450) 상의 사용자들로부터 내부 네

트워크(400)의 자원을 보호하고, 또한 후술되는 특정 영역, 즉 DMZ 내에 있는 서버 및 네트워크 장비 및 자원을 보호하기 위하여, 외부 네트워크(450) 상의 상기 사용자들이 상기 내부 네트워크(400)의 공개되지 않은 자원에 접근하는 것을 막는 역할을 하며, 또한 침입 탐지 및 바이러스 검사, 유해 사이트 차단 등의 기능을 수행한다.

<37> 통합형 보안 게이트웨이(430)는 호스트 대 클라이언트, LAN 대 LAN, LAN 대 클라이언트 가상 사설망(VPN)의 구성을 가능하게 한다. 통합형 보안 게이트웨이(430)는 게이트웨이와 게이트웨이, 게이트웨이와 클라이언트간의 통신에 있어서 데이터를 암호화/복호화할 수 있도록 함으로써 데이터의 비밀성을 보장한다. 상기 통합형 보안 게이트웨이(430)에 의해, IP 주소나 고정 포트별로 별도의 규칙이 부여됨으로써 보다 정교한 패킷 필터링이 가능하며, IP 보안 적용을 위한 데이터의 암호화 및 복호화도 IP 주소 또는 포트별로 가능하다. 또한, 보안 게이트웨이(430)는 IP 보안 적용을 위한 데이터의 암호화시에 적용 가능한 규칙에 따라 서로 다르게 암호화 및 복호화가 가능하고, 스마트 카드에 의해 키 주입 및 변경이 가능하도록 되어 있다.

<38> 통합형 보안 게이트웨이(430)에는 또한 방화벽 기능을 지원하기 위한 프로그램이 구축되어 있다. 통합형 보안 게이트웨이(430)는 응용 프로그램이 방화벽을 통해 외부 네트워크(450)의 호스트(도시되지 않음)와 통신을 하더라도 응용 프로그램이나 외부 서비스 프로그램에 영향을 주지 않는 투명 프록시(transparent proxy) 기능을 제공한다. 프록시 형태로 동작하는 종래의 방화벽은 프록시를 지원하기 위하여 클라이언트 쪽의 해당 응용 프로그램을 수정하거나 방화벽의 특정 포트로 접속하여 새로운 세션(session)을 열어야 하지만, 본 발명은 클라이언트쪽에서 아무런 수정이 필요 없도록 투명 프록시를 지원한다. 또한, 투명 프록시를 지원하기 위해서는 응용 프로그램 별로 처리를 수행할

수 있는 모듈이 있어야 하기 때문에 새로운 응용 프로그램이나 서비스가 생긴 경우에 이를 처리하기 힘든데, 본 발명의 방화벽은 이러한 경우를 위해 관리자가 현재 전송되는 패킷 정보를 이용하여 필요한 정보를 추출하고 이를 규칙에 적용할 수 있도록 되어 있다. 통합형 보안 게이트웨이(430)에도 이러한 응용 프록시를 위한 기능이 제공된다.

<39> 본 발명의 보안 게이트웨이(430)는 상황분석기법(MAC Layer Stateful Inspection)으로서, IP 주소에 의한 정적 패킷 필터링(Static Packet Filtering) 뿐만 아니라 응용 프로그램에 따른 통신 상태에 따라 침입을 탐지할 수 있는 동적 패킷 필터링(Dynamic packet·filtering)을 제공하는데, ASIC칩을 이용하여 하드웨어로 이루어져 있다. 정적 패킷 필터링은 기본적으로 보안 정책에 의해 정해진 규칙에 따라 각 패킷이 검사되어 적절한 동작을 취하도록 되어 있다. 동적 패킷 필터링은 정해진 응용 프로그램의 상태 전이 데이터를 미리 구축해 두고, 이를 바탕으로 현재 들어오거나 나가는 네트워크 패킷이 타당한지를 검사한다. 즉, 이전의 패킷 상태를 이용하여 현재 패킷의 타당성을 검증한다.

<40> 통합형 보안 게이트웨이(430)는 방화벽으로 유효한 URL만 접속을 허용하거나 해당 URL에의 접속을 막기 위한 URL 필터링, 및 네트워크 패킷에 담겨 오는 유해한 정보나, 보안상의 문제점을 노출시킬 수 있는 부분을 필터링하거나 막는 내용 필터링을 제공한다. 내용 필터링은 또한 SMTP(Simple Mail Transport Protocol), FTP, HTTP 필터링을 지원한다. 특히, 자바, 액티브 X, 자바스크립트, VB 스크립트 등의 문제점을 일으킬 수 있는 내용에 대해 필터링을 행한다.

<41> 통합형 보안 게이트웨이(430)는 방화벽으로 비무장 지대와 같은 특정영역인 DMZ(Demilitarized Zone)을 제공하며, 이 DMZ는 내부 네트워크나 외부 네트워크 어디에

도 속하지 않는 네트워크이다. 방화벽의 DMZ는 외부에서 내부 네트워크에 접근할 수 없도록 차단한다. 외부에서는 단지 DMZ 내의 호스트의 서비스만을 이용할 수 있으며, 이를 위해 DMZ 내의 호스트들을 위한 보안 정책을 결정하고 이에 따라 타당한 외부 네트워크에서의 접속만을 허용한다.

<42> 통합형 보안 게이트웨이(430)는 방화벽으로 UDP(User Datagram Protocol) 응용 프로그램 보안을 제공한다. UDP 응용 프로그램은 통신에 있어서 상태 정보를 가지고 있지 않으므로, 보안 문제가 발생할 수 있다. UDP 통신은 요청과 응답 사이의 명확한 구분이 없기 때문에 단순한 패킷 필터링 기법만으로는 패킷을 필터링하기 힘들다. 이를 보완하기 위하여 통합형 보안 게이트웨이의 방화벽은 가상의 세션을 만들어 송수신 관계를 유지한다.

<43> 통합형 보안 게이트웨이(430)는 동적으로 할당되는 포트 보안을 제공한다. RPC(Remote Procedure Call) 기반 서비스는 미리 정의된 포트 번호를 사용하지 않아 단순히 포트 번호를 검색하여 필터링하기가 힘들고, 포트의 할당이 시간에 따라 종종 변하는 등 동적으로 이루어진다. 통합형 보안 게이트웨이(430)의 방화벽은 이를 보완하기 위하여 실행 시간 동안 실행 시간 동안 포트맵퍼(portmapper)로 요청되는 모든 요청을 이용하여 허가된 서비스만 새로운 세션을 만들어 사용 가능하도록 한다.

<44> 통합형 보안 게이트웨이(430)는 방화벽으로 TCP/IP 홀을 이용한 공격을 방지를 제공한다. 일반적으로, TCP/IP 상의 취약한 보안상의 허점을 이용하여 시스템을 공격하거나 다운시킬 수 있으며, 이에 대비하기 위하여 통합형 보안 게이트웨이(430)의 방화벽은 ICMP(Internet Control Message Protocol) 재전송 방지, IP 소스 라우팅의 방지, 정적 라우팅의 사용 등을 지원한다.

<45> 통합형 보안 게이트웨이(430)의 방화벽은 주소 변환 기능(NAT)을 제공한다. 통합형 보안 게이트웨이에서 NAT를 지원하기 위하여 정적 모드와 동적 모드를 지원한다. 정적 모드는 각 내부 네트워크 주소를 각각 타당한 외부 주소에 대응시킨다. 정적 모드는 내부 네트워크에서 외부 네트워크로 통신을 개시할 수 있을 뿐만 아니라, 외부 네트워크에서 내부 네트워크로도 통신을 개시할 수 있다. 동적 모드는 내부 네트워크를 외부로부터 완전히 숨기도록 하여 외부에서 먼저 내부 네트워크로 개시될 수 없도록 한다. 따라서, 동적 모드에서 내부 네트워크는 하나의 외부 주소에 대응될 수 있으며, 내부 네트워크보다 작은 개수의 외부 주소로 대응될 수 있다. 이러한 NAT 기능을 보안 게이트웨이에서 지원하기 위해서 통합형 보안 게이트웨이에서 프록시 arp(address resolution protocol) 서비스를 제공하여 내부 네트워크 주소에 대응되는 외부 네트워크 주소를 자신이 처리할 수 있도록 한다.

<46> 한편, 본 발명의 네트워크 시스템은 또한 도 4에 도시된 바와 같이, 침입 탐지 시스템(Intrusion Detection System)으로서 내장형 또는 외장형의 네트워크 모니터링 시스템(460)을 구비하고 있다. 네트워크 모니터링 시스템(460)은 후술되는 연결 포트(P4)에 연결되는 블랙 존 서버 내에 구현될 수 있으며 내부 및 외부에 노출이 되지 않도록 네트워크 영역에 위치하게 된다. 즉, 통합형 보안 게이트웨이(430)에 병렬 연결되어 있다. 네트워크 모니터링 시스템(460)을 보안 게이트웨이(430)에 병렬 설치함으로써, 본 발명에 있어서 네트워크 모니터링 시스템(460)의 침입 탐지 범위가 'a1 + a2'로 된다. 즉, 네트워크 모니터링 시스템(460)은 상기 라우터(440)에서부터 상기 내부 네트워크(400)까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지할 수 있다. 또한, 상기 네트

워크 모니터링 시스템(460)은 통합형 보안 게이트웨이(430)에 병렬 설치되어 있기 때문에(즉, 네트워크 내부 및 외부에서 탐지되지 않는 네트워크 영역에 위치하기 때문에), 내부 네트워크(400)의 사용자나, 외부 네트워크(450)를 통해 공격을 시도하는 외부 공격자에 의해 탐지되지 않게 된다. 따라서, 확실한 내부 감시를 행할 수 있고, 외부 공격자를 역추적할 수도 있다.

<47> 도 5에는 도 4의 통합형 보안 게이트웨이(430)의 배면도가 도시되어 있다. 도시된 바와 같이, 통합형 보안 게이트웨이(430)는 네트워크 모니터링 시스템(460)과의 연결을 위해 연결 포트(P4)를 구비하고 있다. 또한 통합형 보안 게이트웨이(430)는 내부 네트워크(400)와의 연결을 위한 내부 네트워크 연결 포트(P1)와, DMZ 서버(도시되지 않음)와의 연결을 위한 DMZ 연결 포트(P2)와, 외부 네트워크(450)와의 연결을 위한 외부 네트워크 연결 포트(P3)를 구비하고 있다.

<48> 도 6에는 통합형 보안 게이트웨이(430)에서의 네트워크 패킷의 흐름도가 도시되어 있다. 외부 네트워크(450)로부터 들어오는 입력 패킷은 통합형 보안 게이트웨이(430)를 통해 바로 내부 네트워크(400, 도 4 참조)로 들어갈 수 없고 도 5의 DMZ 연결 포트(P2)에 연결되어 있는 DMZ 서버(470)에 전송되도록 되어 있다. 통합형 보안 게이트웨이의 DMZ 서버(470)에는 방화벽이 구축되어 있으며, 이 방화벽은 상기 입력 패킷이 정당한 패킷인지를 확인하여 상기 입력 패킷을 내부 네트워크(400)로 전송할 것인지를 판단한다. 내부 네트워크(400)로 전송해도 되는 것으로 결정되면, 통합형 상기 보안 게이트웨이(430)에 의해 입력 패킷이 복제되고, 이 복제된 입력 패킷이 도 5의 연결 포트(P4)에 연결된 상기 네트워크 모니터링 시스템(460)에 전송된다.

<49> 네트워크 모니터링 시스템(460)은 복제되어 입력된 상기 입력 패킷이 정당한 패킷

인지 아니면 침입 패킷인지를 판단하고, 판단 결과를 관리자(480)에게 통보한다. 이와 같이, 본 발명에 따라 보안 작업이 이중적으로 수행된다.

<50> 본 발명의 다른 실시예에 따라, 다른 기능을 가진 네트워크 모니터링 시스템을 사용하여 여러 가지 기능을 관리자에게 제공하여 여러 가지 응용에서 호환성을 유지할 수 있다. 예컨대, 본 발명의 네트워크 모니터링 시스템은 통합형 보안 게이트웨이에 병렬로 설치되는 관계로, 내부 및 외부 공격자에 의해 탐지되지 않으므로, 외부 공격자를 역추적할 수도 있다.

<51> 본 발명의 또 다른 실시예에 따라, 블랙 존 서버 내에 구현되는 상기와 같은 네트워크 모니터링 시스템 대신에, 상기 블랙 존 서버 내에 안티 바이러스 시스템이나 유해 사이트 차단 시스템 등을 마찬가지 방법으로 설치하면, 라우터에서부터 내부 네트워크까지의 모든 네트워크 패킷에 대해 바이러스 체크나 유해 사이트 차단 등을 행할 수 있다.

<52> 본 발명의 또 다른 실시예에 따라, 블랙 존에 허브(hub)를 연결하여, 즉 연결 포트(P4)에 허브를 연결하고 이 허브에 네트워크 모니터링 시스템, 안티 바이러스 시스템, 및 유해 사이트 차단 시스템을 연결함으로써 침입 탐지, 바이러스 검사, 및 유해 사이트 차단 등을 수행할 수 있으며, 또한 허브 없이 블랙 존 서버를 통해 상기와 같은 모든 기능을 수행할 수도 있는 등 본 발명은 확장성이 우수하다.

<53> 본 발명은 VPN에서 최고의 성능을 제공하고 또한 일반 네트워크 상에서는 네트워크 구성에 꼭 필요한 게이트웨이로서 게이트 기능, 방화벽 기능, 침입 탐지 기능까지 구현할 수 있다. 또한, 네트워크 모니터링 시스템은 외장형과 내장형으로 구현할 수 있으며, 본 발명의 통합형 보안 게이트웨이는 네트워크 모니터링 프로그램의 능력에 따

라 공격자를 추적하여 역공격까지 가능하다.

【발명의 효과】

<54> 본 발명에 따라 내부 및 외부에서 탐지가 되지 않는 네트워크 영역에 네트워크 모니터링 시스템과 같은 침입 탐지 시스템을 설치함으로써, 내부나 외부로부터의 공격을 회피하면서 라우터에서부터 내부 네트워크까지의 모든 패킷에 대해 침입 여부를 탐지할 수 있고, 방화벽이나 보안 게이트웨이에 대한 공격도 탐지할 수 있기 때문에, 네트워크 시스템에 있어서 보다 완전한 보안을 달성할 수 있다.

<55> 본 발명은 통합형 보안 게이트웨이 등에 의해 필터링된 모든 네트워크 패킷을 확인, 탐지하여 통계 자료를 관리자에게 제공하며, 이에 따라 공격자의 공격 패턴을 알 수 있기 때문에, 그 공격 패턴을 연구함으로써 완전한 보안 정책을 수립할 수 있다.

<56> 또한, 네트워크 모니터링 시스템과 같은 침입 탐지 시스템의 모니터링 능력과 종류에 따라 호환성이 있는 다양한 기능과 서비스를 제공할 수도 있으며, 특히 네트워크 모니터링 시스템 대신에 안티바이러스 시스템을 설치하면, 모든 패킷에 대해 바이러스 검사를 수행할 수 있고, 네트워크 모니터링 시스템과 안티바이러스 시스템 및 유해 사이트 차단 시스템 등을 모두 설치함으로써 보다 완전한 보안 정책을 수립할 수도 있다.

<57> 본 발명은 여러 가지 바람직한 실시예를 참조하여 설명되었지만, 특허청구범위에 설명된 본 발명의 보다 넓은 취지 및 범위로부터 이탈하지 않고 상기 실시예에 대해 각

종 수정이나 변형이 행해질 수 있음은 당업자에게 명백하다.

【특허청구범위】

【청구항 1】

적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와;

상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와;

상기 내부 네트워크와 상기 외부 네트워크를 연결하기 위한 라우터와;

상기 외부 네트워크를 경유한 외부 침입으로부터 상기 내부 네트워크의 자원을 보호하기 위한 방화벽 기능 및 게이트웨이 기능을 제공하기 위하여, 상기 라우터와 상기 내부 네트워크 사이에 설치된 통합형 보안 게이트웨이와;

상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지하는 침입 탐지 수단을 구비하고 있고,

상기 침입 탐지 수단은 내부 및 외부에서 자신의 존재 여부가 탐지되지 않는 네트워크 영역에 위치된 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

【청구항 2】

제 1 항에 있어서,

상기 통합형 보안 게이트웨이는 상기 외부 네트워크로부터의 입력 패킷을 상기 내부 네트워크로 직접 전송하지 않고, 내부의 방화벽 기능에 의해 상기 입력 패킷이 정당 패킷으로 확인될 때 상기 입력 패킷을 복제하여 상기 침입 탐지 수단에 전송함으로써 침입 여부가 이중으로 탐지되도록 한 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

【청구항 3】

제 1 항 또는 제 2 항에 있어서,

상기 네트워크 영역은 상기 통합형 보안 게이트웨이에 병렬 연결됨으로써 형성된 영역인 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

【청구항 4】

적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와;

상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와;

상기 내부 네트워크와 상기 외부 네트워크를 연결하기 위한 라우터와;

상기 외부 네트워크를 경유한 외부 침입으로부터 상기 내부 네트워크의 자원을 보호하기 위한 방화벽 기능, 게이트웨이 기능, 및 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지하는 침입 탐지 기능을 제공하기 위하여, 상기 라우터와 상기 내부 네트워크 사이에 설치된 통합형 보안 게이트웨이를 구비하고 있고,

상기 통합형 보안 게이트웨이의 침입 탐지 기능은 내부 및 외부에서 자신의 존재 여부가 탐지되지 않는 네트워크 영역에서 구현되는 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

【청구항 5】

제 1 항 또는 제 4 항에 있어서,

상기 내부 네트워크는 가상 사설망(VPN)이고,

상기 외부 네트워크는 인터넷인 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

【청구항 6】

제 1 항 또는 제 4 항에 있어서,

상기 통합형 보안 게이트웨이는 내부 및 외부에서 자신의 존재 여부가 탐지되지 않는 네트워크 영역에 위치된 블랙 존 서버를 통해, 또는 허브에 의해 연결된 부가 수단을 통해 침입 차단, 침입 탐지, 바이러스 검사, 유해 사이트 차단을 행하는 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

【청구항 7】

제 1 항 또는 제 4 항에 있어서,

상기 통합형 보안 게이트웨이는 특정 영역(DMZ)에 설치되어 있는 네트워크 장치 및 자원에 대해 외부 침입 차단, 침입 탐지, 바이러스 검사 및 유해 사이트 차단 기능 등을 제공하는 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

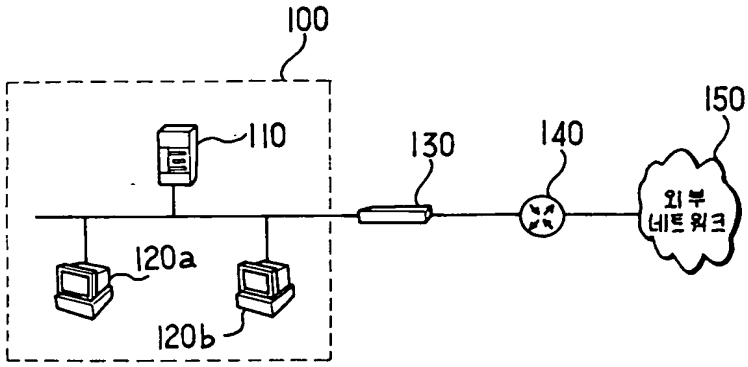
【청구항 8】

제 1 항 또는 제 4 항에 있어서,

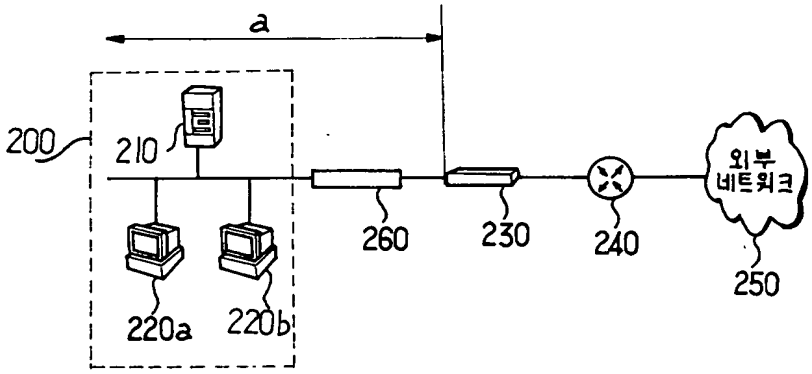
상기 통합형 보안 게이트웨이는 상황분석기법(MAC Layer Stateful Inspection)으로서 IP 주소에 의한 정적 패킷 필터링(Static Packet Filtering) 뿐만 아니라 응용 프로그램에 따른 통신 상태에 따라 침입을 탐지할 수 있는 동적 패킷 필터링(Dynamic packet filtering)을 제공하는데, ASIC칩을 이용하여 하드웨어로 이루어지는 것을 특징으로 하는 통합형 보안 게이트웨이를 구비한 네트워크 시스템.

【도면】

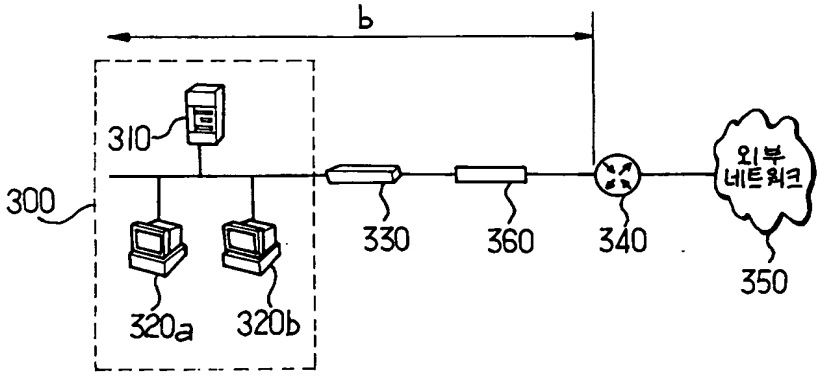
【도 1】


100
110
130
140
150
외부
네트워크
120a
120b

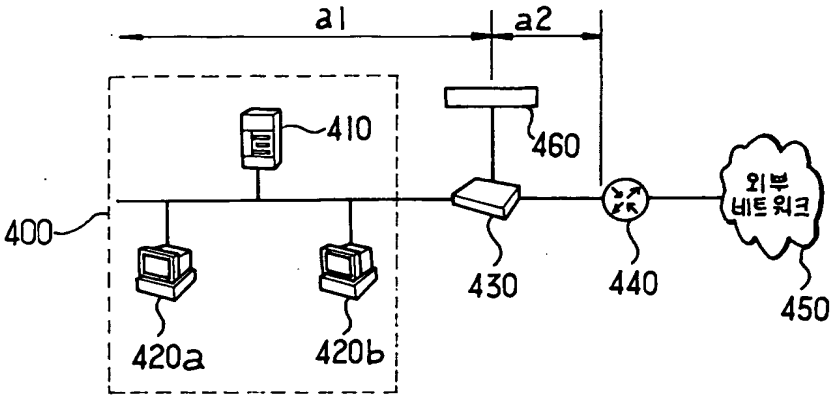
【도 2】


a
200
210
260
230
240
외부
네트워크
250
220a
220b

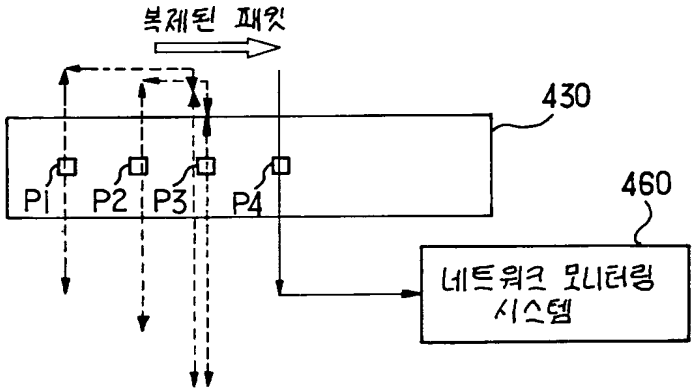
【도 3】


b
310
300
330
360
340
외부
네트워크
350
320a
320b

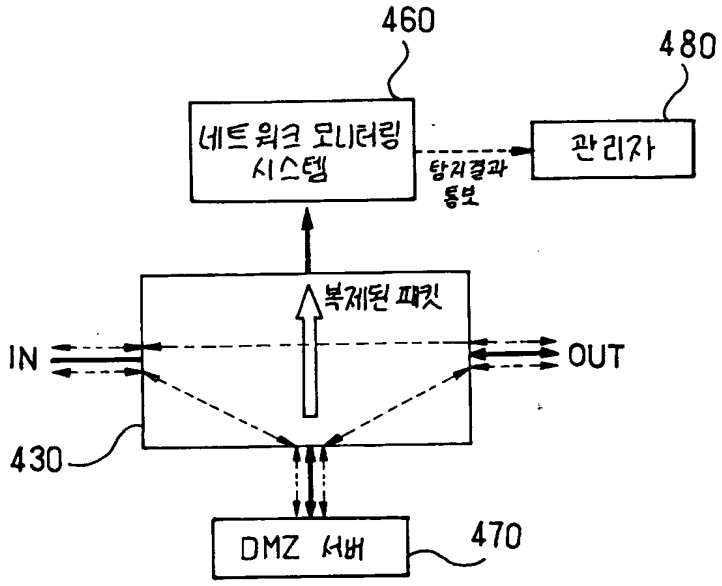
【도 4】


a1
a2
410
460
400
외부
네트워크
430
440
450
420a
420b

【도 5】


복제된 패킷
430
P1
P2
P3
P4
460
네트워크 모니터링
시스템

【도 6】


460
480
네트워크 모니터링
시스템
탐지결과
통보
관리자
복제된 패킷
IN
OUT
430
DMZ 서버
470